

Wednesday, October 10, 2007

SunCEC2007 Day 2: 1st breakout - RBAC by John Walsh

It wasn't the presentation I've expected, but that was my own fault ... reading the abstract before the presentation avoid surprises. I had expected a presentation about Solaris RBAC. Nevertheless the presentation by John Walsh was quite interesting, as it looked to Role Based Access Control from a organisatorial perspective: How to implement Roles? Where are the challenges in doing so?

I took some interesting information out of this breakout.

Often the first try of a customer to implement roles end in role explosion (worstcase: vastly more roles than users)Don't try to put 100% of all roles in your model. The project will never finish80% of the people use 20% of the roles. 20% of the people use 80% of the roles.Based on this observation, define a standard set of roles for the 80% and use exceptions (together with a decent toolset) for the residual 20%There are two methods to determine roles: Top-Down (ask managers about roles) and bottum-up (ask authentication databases about roles). Mostly you end with using both methodologies in a hybrid approach. But whatever you choose to do, choose the methodology that has the least potential of role explosion

Posted by Joerg Moellenkamp in English, suncec2007 at 03:50